The Honorable Robert S. Lasnik

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff v. PAIGE A. THOMPSON, Defendant.	NO. CR19-159 RSL **UNITED STATES' OPPOSITION TO DEFENDANT'S MOTION TO EXCLUDE RULE 404(b) EVIDENCE**

I. INTRODUCTION

Paige Thompson is charged with a scheme to defraud customers who rented cloud server resources from Amazon Web Services (AWS). Her scheme began with scanning approximately 39 million IP addresses hosted by AWS, looking for a specific security vulnerability that would allow her access to internal company servers. Once she found that vulnerability, she used her access to obtain information about IAM roles that had security credentials and permissions to operate in the companies' cloud environments. She then used the IAM roles' security credentials and permissions to (1) steal data from victim companies, and (2) mine cryptocurrency on victim companies' servers using stolen computing power (a practice commonly referred to as "cryptojacking"). The data from Thompson's computer shows that she ran through this same attack vector thousands

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

of times, targeting dozens, if not hundreds, of companies, and refining her technique as she did so. This is a scheme to defraud, as charged in Count 1.

The defense motion to exclude evidence that there were additional, uncharged cryptojacking victims (but not data-theft victims – the defense motion does *not* seek to exclude any data-theft evidence) of Thompson's scheme is based on two mistaken propositions. First, the defense ignores the interconnectedness of Thompson's data-theft and cryptojacking activity, as well as the interconnectedness of Thompson's conduct directed at charged and uncharged victims. Thompson's scheme was to run certain programs over and over and over again, to identify and exploit as many victims as possible. And, she identified and exploited every victim in the same manner: scanning for a vulnerable IAM role, stealing the security credentials associated with that role, and performing certain functions the IAM role was able to perform within the victim's cloud environment. On Thompson's computer, lines of code relating to charged victims are thoroughly intermingled with lines of code relating to uncharged victims.

Because the uncharged victims are part of the same scheme with the same technical foundation, Thompson's uses of their IAM roles are not "other crimes, wrongs, or acts" within the meaning of Federal Rule of Evidence 404(b). *See United States v. Mundi*, 892 F.2d 817, 820 (9th Cir. 1989) (holding that, although the indictment named only one travel agency as a charged victim of a wire fraud scheme, evidence of other uncharged transactions and uncharged victims was admissible as "inextricably intertwined with" the overall scheme); *accord United States v. Loftis*, 842 F.3d 1173, 1178 (9th Cir. 2016). Evidence of Thompson's full attack vector, which included identifying and exploiting the IAM roles of both charged and uncharged victims, is necessary to present a complete, cohesive, and accurate explanation of her scheme. As a result, this evidence is properly admitted without regard to Rule 404(b) and that rule's prescriptions and notice requirement.

Second, even if the evidence were merely Rule 404(b) evidence (rather than inextricably intertwined), the defense conflates the government's proof of Count 1, the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

wire fraud count, with its proof of Count 8, a Computer Fraud and Abuse Act (CFAA) count based on cryptojacking. As to the CFAA count, the government must prove beyond a reasonable doubt that Thompson transmitted a cryptocurrency mining program, code, or command and, as a result of doing so, intentionally caused damage without authorization to a protected computer. But as to the wire fraud count, the government needs only prove that Thompson implemented a scheme to defraud companies, and that one objective of that scheme was to use victim companies' computing power to mine cryptocurrency on her behalf. At trial, the government will prove that Thompson's scheme was successful, meaning that she did, in fact, plant a cryptojacking program on certain victim companies' servers and mine cryptocurrency using stolen computing power. But the Court should reject the defense suggestion that proof of a wire fraud scheme requires the government to prove every aspect of every attack on every victim of the scheme.

In addition, even if the evidence were governed by Rule 404(b), the government provided more-than-sufficient notice. (No such notice is required for inextricably-intertwined evidence.) Under Rule 404(b), the evidentiary threshold for admitting "other acts" evidence under Rule 404(b) is simply whether the totality of the government's evidence would allow a jury to find a particular fact. This is not a high burden, and the government has met it through Thompson's statements alone. The evidence is admissible for a proper purpose, because it is highly probative of Thompson's motive, intent, preparation, and planning, and is not more prejudicial than probative. Because evidence of uncharged cryptojacking victims is inextricably intertwined with Thompson's hacking scheme, and, alternatively, would be admissible under Rule 404(b), the Court should deny Thompson's motion to exclude.

II. FACTUAL BACKGROUND

Evidence of Thompson's hacking scheme comes primarily from two sources: her computer and her own statements. Thompson's computer contains numerous files, folders, file directories, and computer scripts she used to implement her scheme. It also

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

contains notes and command-line logs (that is logs listing some, but not all, commands executed on her computer) that she saved to catalog her efforts. Similarly, Thompson's tweets, internet chats, and texts contain multiple admissions about a large-scale cryptojacking operation that she often referred to as an "enterprise" that gave her a "six-figure salary."

The evidence on Thompson's computer establishes that she took the following steps to hack victim companies. First, she anonymized her Internet identity using both a virtual private network (VPN) and The Onion Router (TOR). Second, she scanned millions of publicly available IP addresses hosted by AWS, looking for web-facing applications with a specific misconfiguration that allowed her to communicate with a company's internal servers.[1]

Third, when she found such misconfigured web applications, she tricked these applications into making internal requests on her behalf. This technique is a variation on a "server-side request forgery," and it is a common form of cyberattack. The request these web-facing applications made on Thompson's behalf was essentially asking if she could access an internal resource on AWS (the instance metadata service), and, if so, requesting internal user data about that resource—including security credentials used to access the resource. The internal user data obtained from the AWS metadata service included the name of the web application's IAM role.[2]

Fourth, once Thompson acquired the name of an application's IAM role, she used the security credentials attached to that role to authenticate into a temporary session with the victim company's internal servers. Fifth, Thompson used the IAM role's permissions to perform actions in the victim company's cloud environment, such as viewing and

---

[1] If these web-facing servers and applications had been properly configured, they would have recognized Thompson's Internet traffic as external and prevented her from accessing internal servers.

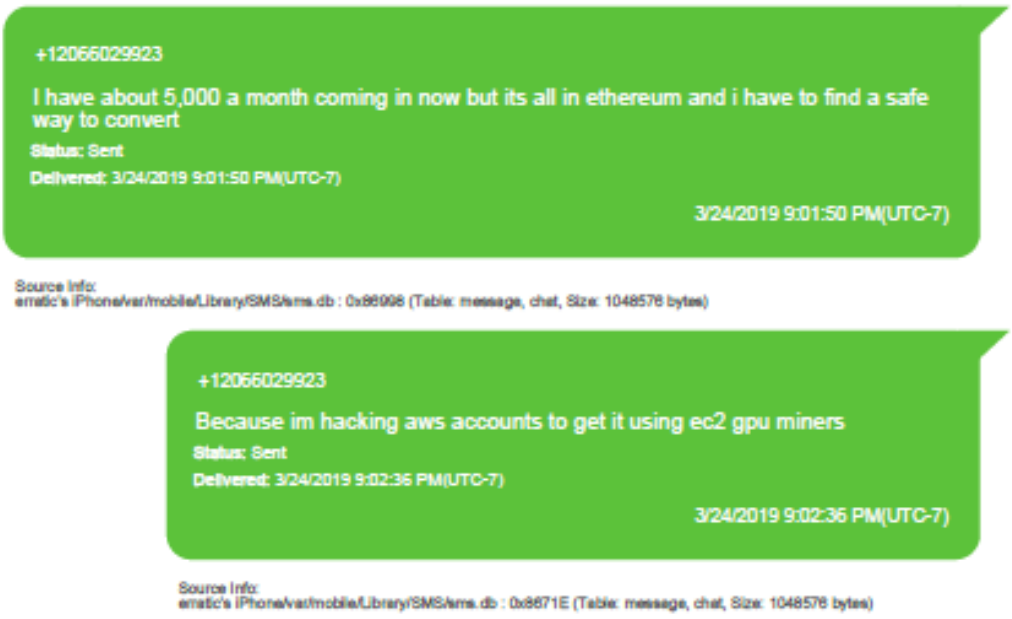
[2] An IAM role is a proprietary AWS product that provides an authorized user with temporary security credentials to perform an authorized function. For example, a company's billing software might be assigned an IAM role that gives it access to records that it needs to perform its billing function.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

copying data, or creating instances (servers), security groups, keypairs, and secured pathways to plant and run cryptocurrency mining programs.

Significantly, Thompson's precise methodology evolved somewhat over time. The evidence on Thompson's computer shows that Thompson often required multiple efforts to accomplish each of the steps described above. Over time, Thompson corrected, improved, streamlined, and automated code to improve upon its functionality or perform additional actions against an AWS server with less manual involvement.

The evidence on Thompson's computer, showing the steps outlined above, is consistent with multiple statements she made online about her cryptojacking activities. For example, she told an associate that she was supporting herself by "hacking ec2 instances and getting access to some aws accounts and using them to mine crypto."[3] In another conversation, she said, "I've straight up gone to my counselor, told her that I was hacking shit and stealing cpu time to mine crypto and buying new things for myself and wearing new designer clothes etc." And then there are these text messages that Thompson sent from her cell phone:



[3] AWS EC2 instances are virtual cloud servers that allow customers to run applications on the AWS cloud infrastructure.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

As shown by both the evidence on Thompson's computer and her own statements, Thompson was engaged in a large-scale scheme to defraud companies by planting software on their servers and using their computing power to mine cryptocurrency. As this Court has already found, evidence of Thompson's cryptojacking scheme is closely intertwined with evidence of her data-theft scheme, because both relied on the same technological foundation. Order Denying Motion to Strike and Sever, pp. 6, 12 (Dkt. 229). Similarly, evidence of uncharged victims is closely intertwined with evidence of charged victims. Throughout Thompson's computer, data pertaining to charged and uncharged victims is commingled in the same relevant files, folders, and file directories because they are all victims of the same fraud.

Attached as Exhibit 1, filed under seal, are excerpts of code found on Thompson's computer. The first four screenshots are portions of logs found on Thompson's computer. Each shows Thompson obtaining IAM roles for both charged and uncharged victims, in rapid sequence. The next three screenshots are portions of logs that show Thompson using those roles to gain access to servers of charged and uncharged victims, again in rapid sequence. The next two screenshots are portions of logs that show Thompson deploying, or attempting to deploy, cryptominers on charged and uncharged victim's servers, again in rapid sequence. The remaining screenshots show that Thompson used the same vector to cryptojack against (1) a named victim and (2) an unnamed victim. As Thompson's scheme evolved, Thompson often first deployed new versions of her malware to attack unnamed victims. As a result, unnamed victims, and evidence relating to them, is necessary to tell the full story of Thompson's criminal conduct.

Even though inextricably intertwined evidence does not implicate Rule 404(b) or its notice requirement, the government provided notice of evidence it intends to introduce regarding additional victims of Thompson's scheme not identified by number in the Second Superseding Indictment. *See* Dkt. No. 242, Ex. A. The government consistently updated that notice to provide the defense with the most up-to-date victim information in

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the government's possession, *see* Dkt. No. 242, Exs. B, C, and, after meeting and conferring with the defense on April 29, 2022, provided a detailed explanation of why the additional evidence is admissible and where in the discovery the evidence can be found, *see id.*, Ex. D. The government thus met Rule 404(b)'s notice requirements, and, even if the evidence of uncharged victims were not inextricably intertwined with the evidence of charged victims, this evidence is admissible to prove Thompson's fraudulent scheme, her motive for hacking AWS accounts, and her intent to defraud.

III. ARGUMENT

A. Evidence of cryptojacking activity against uncharged victims is inextricably intertwined with evidence of cryptojacking activity against charged victims.

As an initial matter, Rule 404(b,) and its notice requirement, applies only to evidence offered under Rule 404(b). "Other acts" evidence that is inextricably intertwined with a charged crime does not need to meet the requirements of Rule 404(b). *United States v. Vizcarra-Martinez*, 66 F.3d 1006, 1012 (9th Cir. 1995). Evidence is inextricably intertwined with a charged crime if it "constitutes a part of the transaction that serves as the basis for the criminal charge," or when other acts are necessary "to permit the prosecutor to offer a coherent and comprehensible story regarding the commission of the crime." *Id.* at 1012-13.

It is well settled that commission of a wire fraud offense requires proof of a fraudulent scheme, and that uncharged acts and transactions can be inextricably intertwined with a such a scheme. *United States v. Lo*, 839 F.3d 777, 793 (9th Cir. 2016); *Loftis*, 843 F.3d at 1177. The Ninth Circuit's decision in *United States v. Mundi* illustrates this point. 892 F.2d 817. In *Mundi*, the defendant was charged with a wire fraud scheme in which he defrauded airlines and travel agencies. *Id.* at 818. Although the superseding indictment named only one travel agency as a victim, the court held that evidence that the defendant's scheme involved other travel agencies was "'inextricably intertwined'" with, and "'part of the same transaction' as, the conduct alleged in the indictment." *Id.* at 820. (The Court held in the alternative that, even if the uncharged

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

transactions had not been inextricably intertwined with the charged scheme, then the evidence was admissible to prove intent under Rule 404(b). *Id.*)

This Court has already found that Thompson's data theft and her cryptojacking activity "relied on the same technical foundation," and that "the cryptomining allegations independently complete a cohesive theory of the government's case." Order Denying Motion to Strike and Sever, p. 6 (Dkt. 229). The Court then reiterated that "the cryptojacking and data theft allegations are closely intertwined because they rely on the same underlying course of action and technical underpinnings." *Id.* at 12. So, too, the evidence of Thompson's cryptojacking of uncharged victims.

It would be impossible for the government to offer the jury a coherent, comprehensible, and accurate explanation of the technical aspects of Thompson's scheme without reference to uncharged victims. Much of the evidence against Thompson is contained on her computer, which was seized from her home and forensically examined by one of the FBI's computer scientists. At trial, that forensic computer scientist will explain the technical aspects of Thompson's scheme, and his testimony relies on the totality of the relevant evidence he reviewed on Thompson's computer. The government's expert cannot base his opinions on part of a computer file, or by looking at some relevant files and not others. This is particularly true, because tracing the evolution of Thompson's scripts necessarily includes references to uncharged victims.

An accurate assessment of Thompson's activity requires analysis of a broad range of files, including files and commands related to uncharged victims. For example, one of the most incriminating files on Thompson's computer is "aws_hacking_shit/aws.commands": a history log, also referred to as a command-line log, in which Thompson saved some of the commands she used to assume victims' IAM roles, steal victim data, and mine cryptocurrency on victim servers. The varying number of commands, deployed against a wide variety of victims, including uncharged victims, provides important information and context for the data and computer scripts found elsewhere on her computer.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The aws.commands file contains thousands of lines of code in which references to charged and uncharged victims are frequently interspersed with one another. *See* Exhibit 1 (filed under seal). In fact, data and computer scripts relating to charged and uncharged victims are commingled in files and file directories throughout Thompson's computer. It is difficult to imagine how evidence could be more inextricably intertwined than lines of code interspersed with one another in a single computer file ("aws_hacking_shit/aws.commands" and "home/erratic/config"), or victim information collected in a single file directory ("aws_dumps", and ".ssh,").

Similarly, Thompsons' statements, which are admissible evidence of her scheme, her motives, and her intent to defraud, do not distinguish between charged and uncharged victims. She frequently told her associates that she was hacking AWS accounts, plural. Her characterization of her cryptojacking activity as an "enterprise" that made several thousand dollars a month suggests that it was a large-scale operation.

As a result, contrary to Thompson's assertion, *see* Dkt. No. 242 at 7, evidence of Thompson's activity directed at uncharged victims is not being advanced by the government to show her propensity for cryptojacking, but, rather because it is—in the most literal sense—inextricably intertwined with, and part of the same transactions as, the conduct alleged in the Second Superseding Indictment. *See Mundi*, 892 F.2d at 820.

B. Evidence of cryptojacking activity is also admissible under Rule 404(b) to prove motive, intent, preparation, and planning.

As the Court knows, Rule 404(b) permits the introduction of "other crimes, wrongs, or acts" when offered to prove "motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake, or lack of accident." Fed. R. Evid. 404(b). This is a rule of inclusion rather than exclusion, meaning that "other acts" evidence is admissible "whenever relevant to an issue other than the defendant's criminal propensity." *United States v. Mehrmanesh*, 689 F.2d 822, 830 (9th Cir. 1982).

In the Ninth Circuit, evidence is admissible under Rule 404(b) if: (1) the evidence tends to prove a material point (that is, the proper purpose); (2) the other act is not too remote in time; (3) the evidence is sufficient to support a finding that the defendant

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

committed the other act; and (4) the act is similar to the offense charged. *United States v. Bailey*, 696 F.3d 795, 799 (9th Cir. 2012).

The defense motion suggests that the only relevant and admissible Rule 404(b) evidence of cryptojacking would be server logs showing cryptocurrency miners running on each and every one of the victim's servers. But the government's ability to present evidence is not so limited. In determining whether evidence is sufficient to support a finding that Thompson was cryptojacking as part of her scheme to defraud—a threshold lower than preponderance of the evidence—a court must consider the totality of the evidence. *Huddleston v. United States*, 485 U.S. 681, 691 (1988). "[I]ndividual pieces of evidence, insufficient in themselves to prove a point, may in cumulation prove it. The sum of an evidentiary presentation may well be greater than its constituent parts." *Id.* (quoting *Bourjaily v. United States*, 483 U.S. 171, 179–180 (1987)).

Here, as explained in the government's 404(b) notices, the low evidentiary threshold is met by a combination of: (1) cryptojacking-related code, programs, and logs on Thompson's computer, (2) social media and text messages in which she admits to cryptojacking, (3) cryptocurrency account records showing that the Ethereum wallet address in Thompson's cryptojacking code actually received cryptocurrency proceeds, and (4) AWS instance and billing records showing that several of a specific kind of AWS EC2 instance with high computing power (the same type of server referenced in Thompson's computer logs) were created on victim AWS accounts, and that the geographic regions of those servers match the logs on Thompson's computer.[4] Exhibit 1 includes representative examples of this evidence.

With respect to the purpose for which this evidence is offered, cryptojacking was an obvious motive for Thompson to hack servers and steal security credentials. This

[4] For example, Thompson's computer logs show that she used one particular victim's IAM role to create p3x16large EC2 instances in the EU-West-1 region (Dublin, Ireland). AWS records show that p3x16large EC2 instances were created in Dublin, Ireland, on the victim's account. Thompson's computer also show that she created a secure shell tunnel (SSH) connection, or backdoor, between her computer and a server linked to the victim's AWS account and IAM role. The government's forensic computer scientist will testify that Thompson deployed her cryptojacking software through these backdoor SSH connections.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

motive is not speculative or circumstantial—it is what Thompson repeatedly said she was doing and why she said she was doing it. Additionally, this evidence also proves Thompson's intent, preparation, planning, and absence of mistake or accident. Thompson did not inadvertently stumble upon victims' internal server information, confidential data, and computing power; rather, she methodically scanned millions of potential victims' servers seeking a specific security flaw. Once she found the security flaw, she exploited it.

Evidence of Thompson's motives and her intent has substantial probative value in this case, not only because intent is an element of wire fraud, but also because Thompson has made her motives and intent a central feature of her defense. At trial, Thompson will assert that she was a "white hat hacker" or good-faith security researcher. But her cryptojacking activity is evidence that she was not acting in good faith; rather, she identified and exploited a security vulnerability for her own personal gain. Thompson is purposefully advancing a defense that is based on a narrow sliver of evidence, while moving to exclude the relevant and admissible evidence that contradicts that defense. Incomplete evidence is the foundation of a misleading narrative. Therefore, even if the government's evidence of uncharged cryptojacking victims were for some reason otherwise inadmissible under Rule 404(b), Thompson's defense strategy would open the door to it.

For the same reasons, evidence of uncharged cryptojacking victims easily passes Rule 403's balancing test. The evidence is highly probative because it bears on a hotly contested issue at trial. Far from being prejudicial or misleading, a comprehensive presentation of Thompson's scheme is necessary to avoid misleading the jury.

C. The government provided more than sufficient notice under Rule 404(b).

Rule 404(b) was recently amended to require the prosecution to provide "reasonable notice" of its intent to offer such evidence in criminal cases. Fed. R. Evid. 404(b)(3) (2020). The prosecution's notice must articulate "the permitted purpose for

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

which the prosecutor intends to offer the evidence and the reasoning that supports the purpose." *Id.*

The government has provided the defense with a series of detailed Rule 404(b) notices that far exceed what is required under the rule. First, in January 2020, the government gave the defense a presentation about Thompson's hacking methodology that included a section on her cryptojacking exploits. *See* Dkt. No. 131, Ex. A (sealed). Then, in response to a defense discovery request in April 2021, the government prepared and provided an expert report describing the evidence of cryptojacking, along with a file directory explaining where that evidence could be located on Thompson's computer. *See* Dkt. No. 242, Ex. D, pp. 9-25. And, in February 2022, the government produced a 32-page expert report describing the forensic analysis of Thompson's cryptocurrency mining programs. Exhibit 2 (filed under seal).

Between December 2021 and March 2022, the parties litigated the issue of whether the cryptojacking allegations should be stricken from Count 1, and whether the cryptojacking count (Count 8) should be severed from the remaining counts in the Indictment. *See* Dkt. Nos. 124, 138, 163, 175, 184. In its order denying Thompson's motion, this Court summarized the allegations in Count 1 and observed that both the data theft and cryptojacking allegations "relied on the same technical foundation, and the indictment makes this abundantly clear." Order Denying Motion to Strike and Sever, pp. 5-6 (Dkt. No. 229).

On March 11, 2022, the government filed a Bill of Particulars identifying the charged cryptojacking victims as Victims 7 and 8. Dkt. No. 210. The Bill of Particulars states, "[T]he government has provided defense counsel a letter that identifies additional data theft and cryptojacking victims . . . and notes that the government intends to introduce evidence concerning these victims and that such evidence is admissible, both because it is inextricably intertwined with the charged conduct, and pursuant to Federal Rule of Evidence 404(b)." Dkt. No. 210 at 4-5. The March 11 letter explained that the government was offering evidence of uncharged data theft and cryptojacking victims

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

"because it shows that your client scanned millions of potential victims' computers seeking security flaws, rather than inadvertently discovering and/or taking information that she did not realize belonged to others." Dkt. No. 242, Ex. A at 3. The government further explained that the number of victims rebutted any claim that Thompson attempted to notify victims of security flaws, and that she had a financial motive for exploiting the security flaws she found. *Id.* The government identified four uncharged cryptojacking victims on March 11, and another five uncharged cryptojacking victims on April 22. *See* Dkt. No. 242, Ex. B.

In an April 27 letter, followed by a conference call two days later, the defense stated that it believed the government's notice was insufficient because it did not identify discovery showing that Thompson planted cryptocurrency-mining software on the servers of uncharged victims. *See* Dkt. No. 242, Ex. C. The government responded on May 6 with another letter specifically identifying the evidence (including by specific Bates range) the government intended to introduce in support of its cryptojacking allegations. *See* Dkt. No. 242, Ex. D. In that letter, the government pointed to folder names, file paths, discussion of relevant code, social media messages, cryptocurrency records, IP addresses, IAM roles, account numbers, and billing records all produced to the defense. *See id.*

As shown by the foregoing, the government has been extremely detailed in its explanation of Thompson's hacking scheme and the evidence it intends to present in support of that scheme. Whatever objections the defense may have to the admissibility of this evidence, lack of reasonable notice cannot be among them.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

IV. CONCLUSION

For the foregoing reasons, the Court should deny Thompson's motion.

DATED: May 20, 2022.

Respectfully submitted,

NICHOLAS W. BROWN
United States Attorney

/s Andrew C. Friedman
/s Jessica M. Manca
/s Tania M. Culbertson
ANDREW C. FRIEDMAN
JESSICA M. MANCA
TANIA M. CULBERTSON
Assistant United States Attorney
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
Telephone: (206) 553-7970
Fax: (206) 553-0882
E-mail: Andrew.Friedman@usdoj.gov
Jessica.Manca@usdoj.gov
Tania.Culbertson@usdoj.gov